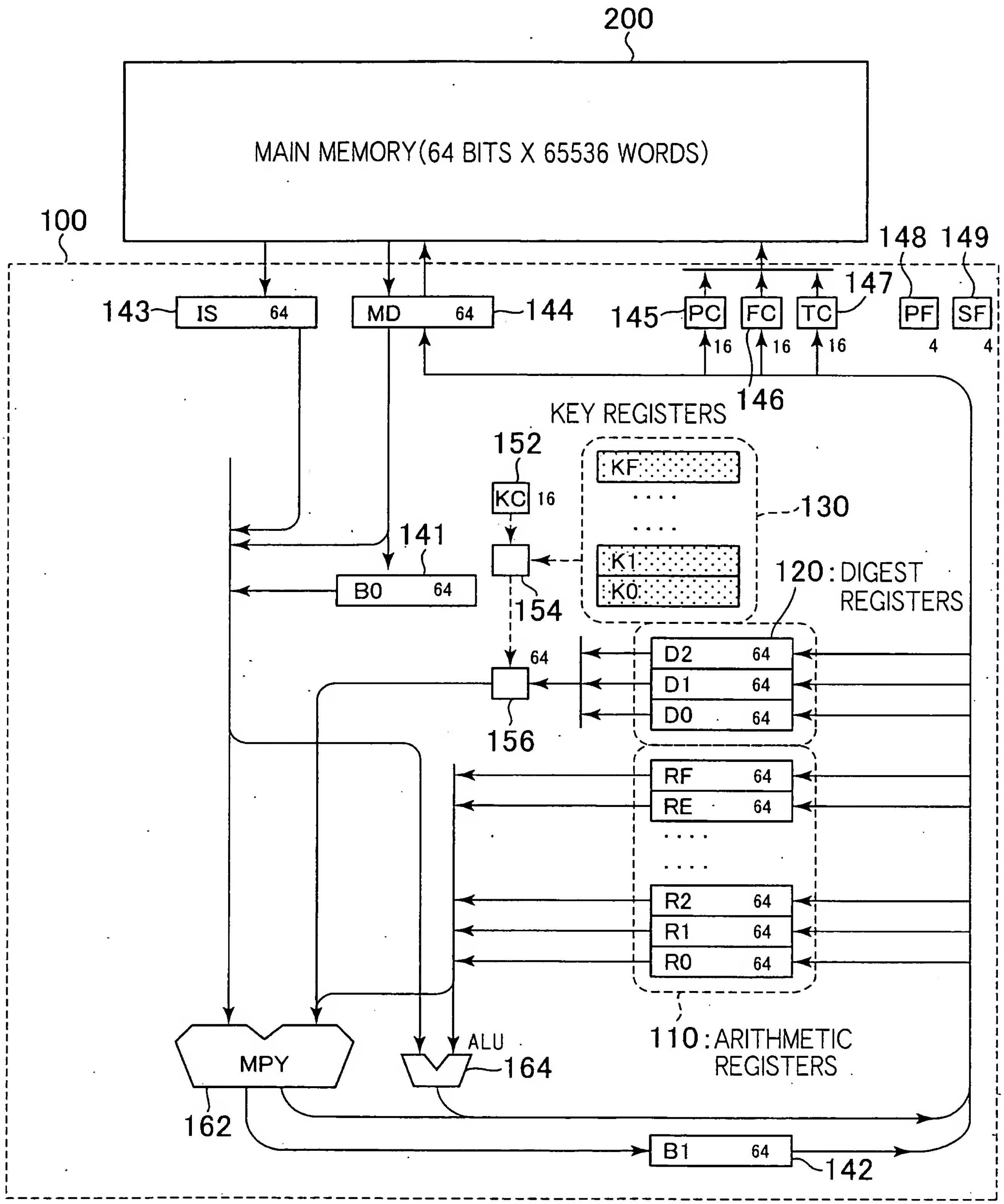
200
MAIN MEMORY(64 BITS X 65536 WORDS)
100
148 149
147
143
IS 64
MD 64
144
145
PC
FC
TC
PF
SF
16
16
16
4
4
146
KEY REGISTERS
152
KC 16
KF
130
141
B0 64
K1
K0
154
120: DIGEST REGISTERS
64
D2 64
D1 64
D0 64
156
RF 64
RE 64
R2 64
R1 64
R0 64
110: ARITHMETIC REGISTERS
MPY
ALU
164
162
B1 64
142

FIG. 1

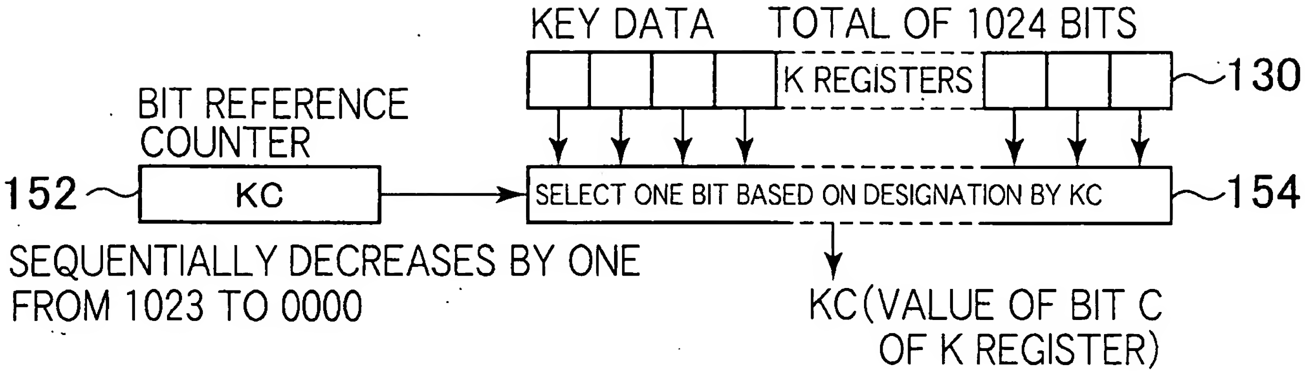
KEY DATA
TOTAL OF 1024 BITS
K REGISTERS
130
BIT REFERENCE COUNTER
152
KC
SELECT ONE BIT BASED ON DESIGNATION BY KC
154
SEQUENTIALLY DECREASES BY ONE FROM 1023 TO 0000
KC(VALUE OF BIT C OF K REGISTER)

FIG. 2

NAME	BIT LENGTH	DESCRIPTION	
OP	4	Operation Code	OP CODE
SOP	4	Sub-Operation Code	OP EXTENSION CODE
MF	4	Mode F Operand	F OPERAND ADDRESS MODE
MT	4	Mode T Operand	T OPERAND ADDRESS MODE
L	16	Length	LENGTH OF T, F, AND S OPERAND *1
F	16	From Operand (F Operand)	F OPERAND
T	16	To Operand (T Operan)	T OPERAND
S	16	Sink Operand (S Operand)	S OPERAND *2

*1 DOUBLE WORD

*2 ONLY MULTIPLE LENGTH
MULTIPLICATION INSTRUCTION

FIG. 3(a)

OPERAND DESIGNATION MODE	BINARY CODE	DESCRIPTION OF MODE
D	0000	INTERPRET VALUE OF F OR T OPERAND AS ARITHMETIC REGISTER NUMBER AND ACCESS CONTENT OF THAT REGISTER (DIRECT REGISTER DESIGNATION)
I	0001	INTERPRET VALUE OF F OR T OPERAND AS ARITHMETIC REGISTER NUMBER AND ACCESS MEMORY USING CONTENT OF THE REGISTER AS ADDRESS (INDIRECT REGISTER DESIGNATION)
A	0010	INTERPRET VALUE OF F OR T OPERAND AS ADDRESS AND ACCESS MEMORY ACCORDING TO THAT ADDRESS (DIRECT ADDRESS DESIGNATION)
IP	0011	CONDUCT INDIRECT REGISTER DESIGNATION AND THEN INCREASE ACCESSED REGISTER VALUE BY ONE
MI	0100	DECREASE DESIGNATED REGISTER VALUE BY ONE AND THEN ACCESS MEMORY USING THE RESULTING VALUE AS ADDRESS
IV16	0101	DIRECTLY USE 16-BIT VALUE DESIGNATED IN F OPERAND FOR CALCULATION
IV64	0110	DIRECTLY USE 64-BIT VALUE DESIGNATED IN NEXT INSTRUCTION FOR CALCULATION
LI	1000	INDIRECT REGISTER DESIGNATED DOUBLE LENGTH CALCULATION MODE. CALCULATE DOUBLE LENGTH DATA DESIGNATED IN L FIELD USING CONTENT OF REGISTER DESIGNATED BY F OR T OPERAND AS START ADDRESS OF DOUBLE LENGTH DATA
LA	1001	DIRECT ADDRESS DESIGNATED DOUBLE LENGTH CALCULATION MODE. CALCULATE DOUBLE LENGTH DATA DESIGNATED IN L FIELD USING ADDRESS DESIGNATED BY F OR T OPERAND AS START ADDRESS OF DOUBLE LENGTH DATA

FIG. 3(b)

OP (4bit)	SOP (4bit)	MF (4bit)	MT (4bit)	L (16bit)	F (16bit)	T (16bit)	MNEMONIC	OPERATION	PSW (N Z V C)	ATTRIBUTE
0000		D	D				HLT	HLT		
0001	0000	D	-ttt			T	CLR	0 → T	0100	
0001	0001						CLRS		0100	
0010	0000	D	-ttt			T	ASL	T × 2 → T	**0*	SFTs
0010	0001	D	-ttt			T	ASR	T ÷ 2 → T	**0*	
0010	0010	D	tttt	L		T	LSL	SHIFT T LEFT LOGICALLY → T	**0*	
0010	0011	D	tttt	L		T	LSR	SHIFT T RIGHT LOGICALLY → T	**0*	
0010	0100	D	tttt	L		T	LSLC	SHIFT T LEFT LOGICALLY → T (INCLUDING CARRY)	**0*	
0010	0101	D	tttt	L		T	LSRC	SHIFT T RIGHT LOGICALLY → T (INCLUDING CARRY)	**0*	
0010	0110	D	-ttt			T	RSL	ROTATE T LEFT → T	**0*	
0010	0111	D	-ttt			T	RSR	ROTATE T RIGHT → T	**0*	
0011	0000	ffff	tttt	L	F	T	ADD	T+F → T	****	ADDs
0011	0001	ffff	tttt	L	F	T	ADC	T + F + Cflag → T	****	
0011	0010	ffff	tttt	L	F	T	INC	T + 1 → T	****	
0011	0011	D	-ttt			T	NEG	¬T + 1 → T	****	
0100	0000	ffff	tttt	L	F	T	SUB	T - F → T	****	SUBs
0100	0001	ffff	tttt	L	F	T	SBB	T - F - Cflag → T	****	
0100	0010	ffff	tttt	L	F	T	DEC	T - 1 → T	****	
0100	0011	ffff	tttt	L	F	T	CMP	T - F → T	****	
0101	0000	ffff	tttt	L	F	T	AND	T∧F → T	**0-	BITs
0101	0001	ffff	tttt	L	F	T	OR	T∨F → T	**0-	
0101	0010	ffff	tttt	L	F	T	XOR	T∀F → T	**0-	
0101	0011	ffff	tttt	L	F	T	NOT	¬T → T	**0-	
0101	0100	-fff	-ttt		F	T	BIT	T∧F → T	**0-	
0110	0000	ffff	tttt	L	F	T	MOV	F → T	**0-	MOVs
0110	0001	-fff	IP		F	SP	PUSH	F → (SP)+		
0110	0010	MI	-ttt		SP	T	POP	-(SP) → T		
0110	0011	-fff	D		F	?	IN	F → ?		
0110	0100	D	-ttt		F	?	OUT	? → T		
0111	0000	-fff	D		F	PC	JMP	F → PC		JMPs
0111	0001	-fff	D		F	PC	RJP	PC + F → PC		
0111	0010	MI	D		SP	PC	RET	-(SP) → PC		
0111	0011	MI	D		SP	PC	RIT	-(SP) → PC, ITF reset		
1000	0000	-fff	D		F	PC	JSR	PC → (SP)+, F → PC		LINKs
1000	0001	-fff	D		F	PC	RJS	PC → (SP)+, PC + F → PC		
1000	0010	-fff	D		F	PC	SVC	PC → (SP)+, F → PC, ITF set		
1001	0000	-fff	D		F	PC	BRN	[N=1] F → PC		BRs
1001	0001	-fff	D		F	PC	BRZ	[Z=1] F → PC		
1001	0010	-fff	D		F	PC	BRV	[V=1] F → PC		
1001	0011	-fff	D		F	PC	BRC	[C=1] F → PC		
1010	0000	-fff			F	PC	LOOP	(PC)-1→(PC) [Z≠1] F→PC	-*--	
1010	0001	ffff	D	0011	F		DMV	F(DIGEST)→ (D0,D1,D2)		
1010	0010	-fff	tttt		F	T	XCHG	F → T, T → F		
1011	0000	-fff	-ttt		F	T	MUL	F × T→RF,RE	****	
1100	0000	D	D			PC	SIG	PC → (SP)+, FIXED ADDRESS→PC,SF$_{set}$ INITIALIZE KC		LINKs
1100	0001	MI	D		SP	PC	SIE	[SF=1,KC=0]-(SP)→PC, SF reset		JMPs
1100	0010	-fff	D		F		KCJ	[SF=1·KCE≠0] F → PC		
1100	0011	LA	LA	L	F	T	ADO	[SF=1] F+T+1→T		
1100	0100	LA	LA			T	SCMP	[SF=1] compare N with T		ROMs
1100	0101	LA	LA			T	SSB	[SF=1]T-N→T		ROMs

FIG. 4-1 (a)

OP (4bit)	SOP (4bit)	L (8bit)	F (16bit)	T (16bit)	S (16bit)	MNEMONIC	OPERATION	PSW	
1101	0000	L	F	T	S	MLS	[SF=1] F × T→S		MULs
1101	0001	L		T	S	MDK	[SF=1] T × D^{Kc}→S,KC−1→KC		
1101	0010	L		T	S	MLD	[SF=1] T × D→S		
1101	0011	L		T	S	MLL	[SF=1] N'(rom) × Tの下位→S		
1101	0100	L		T	S	MLH	[SF=1] N(rom) × Tの上位→S		
1101	0101	L		T	S	MLP	[SF=1] CONSTANT R^2modN(rom) × T→S		

FIG. 4-2(b)

DESCRIPTION OF FIELD AND SYMBOL

FIELD	SYMBOL	DESCRIPTION
MF,MT *1,*2	D	FIXED TO D MODE. BINARY CODE CORRESPONDING TO D MODE IS SET.
	IP	FIXED TO IP MODE. BINARY CODE CORRESPONDING TO IP MODE IS SET.
	MI	FIXED TO MI MODE. BINARY CODE CORRESPONDING TO MI MODE IS SET.
	LA	FIXED TO LA MODE. BINARY CODE CORRESPONDING TO LA MODE IS SET.
	LI	FIXED TO LI MODE. BINARY CODE CORRESPONDING TO LI MODE IS SET.
	f	ARBITRARY BIT IS DESIGNATED.
	t	ARBITRARY BIT IS DESIGNATED.
	-	NO DESIGNATION. IGNORE EVEN IF DESIGNATED.
L	L	LENGTH OF ARBITRARY DOUBLE LENGTH DATA IS DESIGNATED.
	0011	FIXED LENGTH OF TRIPLE LENGTH DATA (64 X 3) IS DESIGNATED.
F,T	F	REGISTER NUMBER OR ADDRESS, AND DATA ARE DESIGNATED. MEANING CHANGES ACCORDING TO MODE. *2
	T	REGISTER NUMBER OR ADDRESS, AND DATA ARE DESIGNATED. MEANING CHANGES ACCORDING TO MODE. *2
	PC *3	PROGRAM COUNTER (PC) REGISTER IS DESIGNATED.
	SP	STACK POINTER (SP) REGISTER IS DESIGNATED.
	?	NOT DESIGNED. DESIGNATION TARGET IS NOT DECIDED.
S	S	UPPER SPECIFIC ADDRESS OF MAIN MEMORY IS DESIGNATED.
PSW	*	DON'T CARE (EITHER 1 OR 0 IS SET)
	-	NOT USED
	0	0 IS FIXED.
	1	1 IS FIXED.

FIG. 4-2(c)

DESCRIPTION OF OPERATIONS

SYMBOL	DESCRIPTION
∨	AND OPERATION
∧	OR OPERATION
⊻	XOR OPERATION
¬	NOT OPERATION
(~)	INDIRECTLY ACCESS VALUE OF ~ *4
(~)+	INDIRECTLY ACCESS VALUE OF ~ AND INCREASE IT BY ONE
−(~)	DECREASE VALUE OF ~ BY ONE AND ACCESS IT INDIRECTLY
[~]	USE ~ AS CONDITION

FIG. 4-2(d)

NOTE
*1: A MODE MAY BE DESIGNATED EVEN THOUGH F OR T OPERAND CANNOT BE ARBITRARILY DESIGNATED. THIS IS BECAUSE EVEN THOUGH REGISTER OR ADDRESS IS NOT DESIGNATED, THE SAME OPERATION AS THAT IN DESIGNATED MODE IS NECESSARY FOR CONTROL. E.G., HLT AND ASL.
*2: SEE 'DESCRIPTION OF MODE' IN THE NEXT PAGE FOR DESCRIPTION OF MODE DESIGNATION.
*3: ALTHOUGH STACK POINTER (SP) IS NOT SHOWN IN SEP-4 BLOCK DIAGRAM, IT EXISTS.
*4: INDIRECT ACCESS DENOTES TO ACCESS MEMORY USING CONTENT OF REGISTER AS ADDRESS AND ACCESS VALUE STORED IN THE ADDRESS.
*5: L FIELD AND F, T, AND S OPERAND IN INSTRUCTIONS WITH CONDITION OF 'SF = 1' CAN BE USED FOR SPECIFIC ADDRESS THAT IS USED IN SIGNATURE CALCULATION.

FIG. 4-2(e)

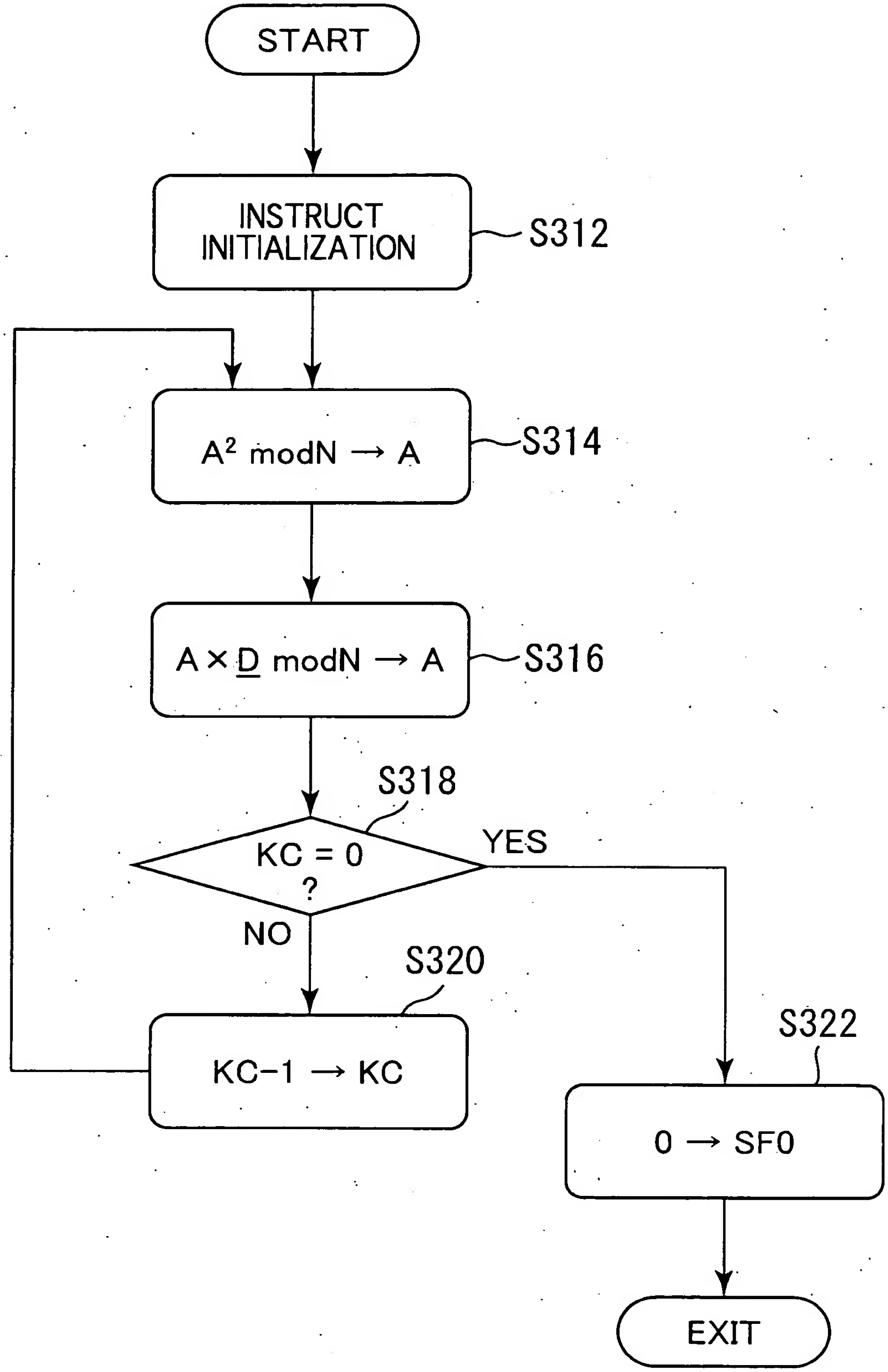
START
INSTRUCT INITIALIZATION
S312
A^2 modN → A
S314
A × D modN → A
S316
S318
KC = 0 ?
YES
NO
S320
KC−1 → KC
S322
0 → SF0
EXIT

FIG. 5

PROCEDURE		INSTRUCTION	OPERATION	NOTE	
(01)	AR*	MLP	R* × A → Z	ZH DENOTES UPPER 1024 BITS OF Z WHILE ZL DENOTES LOWER 1024 BITS THEREOF. CALCULATION THEREOF IS NOT NECESSARY.	THIS IS EQUIVALENT TO SUBSTITUTING R^2 mod N FOR X AND A FOR Y IN FUNCTION "XYR^{-1}mod N"
(02)	AR* mod R				
(03)	(02) × N*	MLL	LOWER 1024 BITS OF 'N* X ZL' → U	PROCESSING OF (03) AND (04) IS PERFORMED AT ONCE USING MLL.	
(04)	(03) mod R				
(05)	(04) × N	MLH	UPPER 1024 BITS OF 'N X U' → AC	UPPER BITS OF '(04) X N' ARE ACTUALLY NEEDED FOR (06). LOWER BITS CAN BE NEGLECTED.	
(06)	(01) + (05)	ADO	ZH + AC + 1 → AC	PROCESSING OF (06) AND (07) IS PERFORMED AT ONCE USING ADO. THIS IS BECAUSE 'ZH + AC + 1' IS ALWAYS MULTIPLE OF R.	
(07)	(06) / R				
(08)	(07) − N	SCMP	COMPARE AC AND N	COMPARISON RESULTS REFLECT ON NEXT INSTRUCTION.	
		SSB	[AC > N] AC − N → AC	WHETHER TO SUBTRACT N IS DETERMINED ACCORDING TO COMPARISON RESULTS. VALUE OF AC BECOMES "AR^2modN"	
(09)	(08) × D	MDK	AC × D^{kc} → Z	ZH DENOTES UPPER 1024 BITS OF Z WHILE ZL DENOTES LOWER 1024 BITS THEREOF. CALCULATION THEREOF IS NOT NECESSARY.	THIS IS EQUIVALENT TO SUBSTITUTING AR FOR X AND D FOR Y IN FUNCTION "XYR^{-1}mod N"
(10)	(09) mod R				
(11)	(10) × N*	MLL	LOWER 1024 BITS OF 'N* X ZL' → U	PROCESSING OF (11) AND (12) IS PERFORMED AT ONCE USING MLL.	
(12)	(11) mod R				
(13)	(12) × N	MLH	UPPER 1024 BITS OF 'N X U' → AC	UPPER BITS OF '(12) X N' ARE ACTUALLY NEEDED FOR (14). LOWER BITS CAN BE NEGLECTED.	
(14)	(09) + (13)	ADO	ZH + AC + 1 → AC	PROCESSING OF (14) AND (15) IS PERFORMED AT ONCE USING ADO. THIS IS BECAUSE 'ZH + AC + 1' IS ALWAYS MULTIPLE OF R.	
(15)	(06) / R				
(16)	(14) − N	SCMP	COMPARE AC AND N	COMPARISON RESULTS REFLECT ON NEXT INSTRUCTION.	
		SSB	[AC > N] AC − N → AC	WHETHER TO SUBTRACT N IS DETERMINED ACCORDING TO COMPARISON RESULTS. VALUE OF AC BECOMES "AD mod N"	

FIG. 6(a)

SYMBOL	MEANING OF SYMBOL
R*	CONSTANT: R^2 mod N
R	CONSTANT: R
N	CONSTANT: N
N*	CONSTANT: VALUE SATISFYING NN* mod R = R - 1
A	ARBITRARY VALUE
D	DIGEST
Z	TEMPORARY VARIABLE. 2048 BITS.
ZH	UPPER 1024 BITS OF Z
ZL	LOWER 1024 BITS OF Z
U	TEMPORARY VARIABLE. 1024 BITS.
AC	ACCUMULATED INTERMEDIARY RESULTS. 1024 BITS.

FIG. 6 (b)

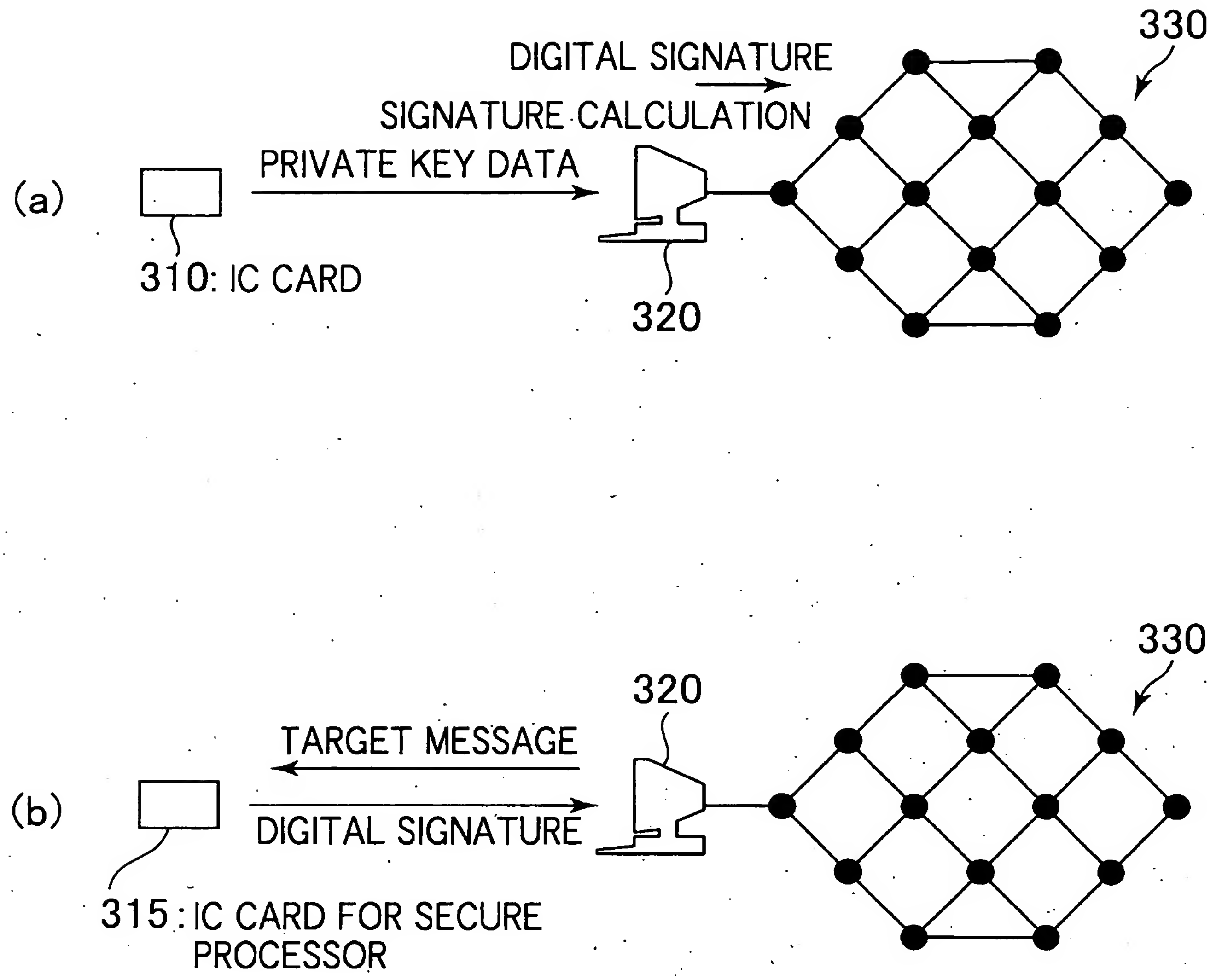
330
DIGITAL SIGNATURE
SIGNATURE CALCULATION
PRIVATE KEY DATA
(a)
310: IC CARD
320
330
320
TARGET MESSAGE
(b)
DIGITAL SIGNATURE
315: IC CARD FOR SECURE PROCESSOR

FIG. 7